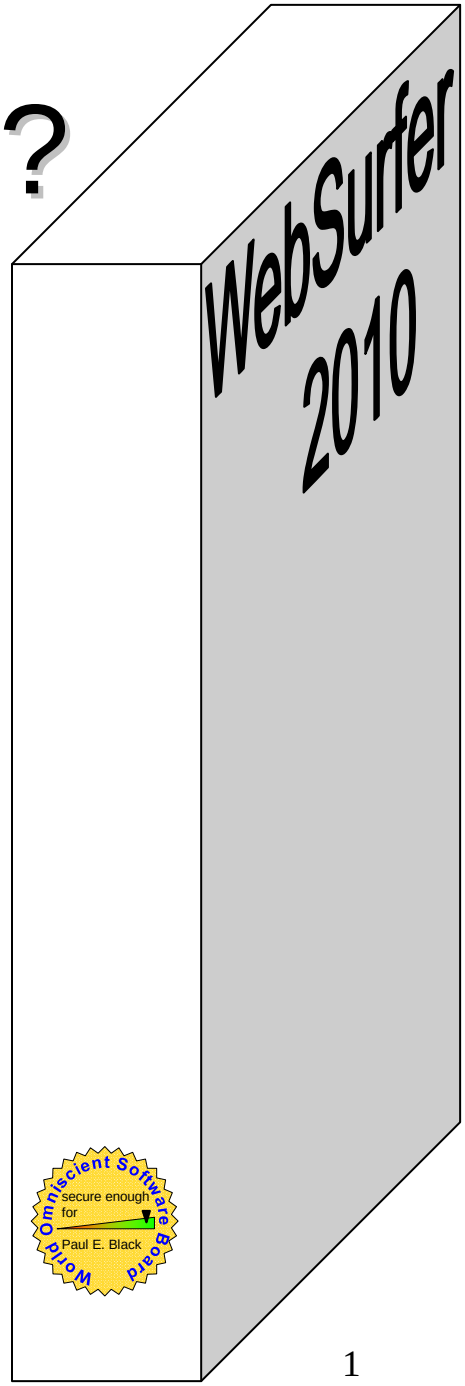
Wouldn't it be Nice …?



What are the Goals?

- **Inform “buy” decision**
- **Convey secure settings**
- **Feed confidence and assessments**
- **Lead to more secure software**

- **Contact**
  - **Daniel G. Wolf**
    - **Software Assurance Consortium**
  - **Paul E. Black**
    - **NIST**

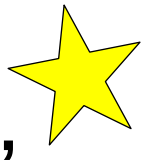
Possible Content: People/Process

- **People**
  - **Is there code accountability or responsibility assigned?**
  - **Is there a trained, certified, or accredited application security “Software Engineer”?**
- **Process**
  - **Secure coding practices followed**
  - **Was a threat model defined?**
  - **Are there requirements?**
  - **Testing methodology**
    - **Black box, unit security testing, penetration testing, …**
  - **Tested on what platforms?**
  - **Code reviewed? other than by developers? for security?**
  - **Static analysis**

Possible Content: Software Itself

- **Pedigree: amount from libraries, from Open Source, compiler**
- **Design: encryption, single points of failure, architecture signed off by app sec certified software engineer**
- **Provenance: protection of code in supply chain**
- **Traits: all communication over SSL, uses Internet or email**
- **Size: lines of code, function points, number of modules**
- **What and where are configuration files?**
- **% “banned” APIs, # “unforgivable vulnerabilities”**

Audiences & Scope



1. **Small businesses (dentist, dry cleaner, accountant, plumber, restaurant)**
   - **General applications running on general purpose hardware (accounting package on a "PC")**
2. **Integrators (incoming software is just one piece)**
3. **Naïve home users (my brother)**
   - **General applications (not OS or security-specific)**